I claim:

1. A process for securing information in a digital form comprising:
   - creating an identifier using information obtained from a device capable of rendering the digitized information to be secured;
   - associating the identifier with the information to be rendered;
   - securing said digitized information by preventing the rendering of the information if the identity of the device upon which the information is to be rendered is not verified using said identifier.

2. A process according to claim 1 wherein the identifier is a binary key suitable for use in an algorithm that can secure said digitized information.

3. A process according to claim 2, wherein the identifier is produced by evaluating information associated with a specific physical device that can render the secured information and the identifier uniquely identifies said device.

4. A process according to claim 2, wherein the identifier is produced by evaluating information associated with a class of physical devices that can render the secured information and the identifier uniquely identifies said class of devices.

5. The process as set forth in claim 2, wherein the information associated with the specific physical device that is to be used to render the secured information is produced by:
   - obtaining information representing a physical or functional attribute of at least one component in said physical device which is unique to that component; and
   - converting said information into a binary key by performing a cyclic redundancy check or other repeatable process on said information.

6. A process according to claim 5, wherein the identifier comprises a binary key of at least 64 bits in length.

7. A process according to claim 6, wherein the information is secured by preventing the rendering of the information by the device on the basis of information produced by a test for authentication of the device using the said binary key and an algorithm suitable for authentication.

8. A process according to claim 6, wherein the information is secured by preventing the operation of the device on the basis of information produced by a test for authentication of the device using the said binary key and an algorithm suitable for authentication.

9. The process as set forth in claim 7 wherein the test for authentication comprises comparing information associated with the data to be rendered with information produced by an evaluation of the device which is to be used to render said data.

10. The process as set forth in claim 9 wherein the evaluation of the device occurs during the process of authentication.

11. The process as set forth in claim 9 wherein the information to be rendered is received by the device in an encoded format, and is unencoded prior to rendering by said device.

12. The process as set forth in claim 9 wherein the information to be rendered is received by the device in an encoded format distinct from a format that the device can use to render said information, and said information is unencoded prior to rendering by said device.

13. The process as set forth in claim 9 wherein the information to be rendered is received by the device in a format the device can render without subsequent transformation.

14. The process as set forth in claim 6 wherein the physical device is a general purpose computer and the component is selected from the group consisting of a bus, a microprocessor, an integrated circuit, a hard drive; a video display circuit, a network interface circuit, a video display card, a network interface card or a circuit located on a peripheral connected to a local bus on said system.

15. A process for securely transferring information in a digital form comprising:

- obtaining information to be distributed, wherein the information is in a digital form;
- producing a binary key of at least 64 bits using information associated with the device that is to render the information after it has been distributed;
- encoding the information by using the unique identifier in combination with an algorithm suitable for encoding such information;
- transferring the information to the location at which the device that is to render the information is located;
- decoding the information by
    - producing a binary key by collecting information from the device that is to render the information after receiving the information;
    - decoding the encoded information using the binary key.

16. The process as set forth in claim 15, wherein the steps of decoding the encoded information are performed incidental to the process of rendering the information.

17. The process as set forth in claim 15, wherein the device used in rendering the information produces the key incidental to the process of decoding and rendering the encoded information.

18. The process as set forth in claim 15, wherein the steps of decoding the encoded information are performed by a distinct device from the device that renders the information.

19. The process as set forth in claim 15, wherein the steps of decoding the encoded information are performed by the device that renders the information.

20. The process as set forth in claim 15, wherein the key is associated with the data containing the encoded information.

21. The process as set forth in claim 15, wherein the key is transferred distinct from the file containing the encoded information.

22. The process as set forth in claim 15, wherein the process further comprises:

- segmenting the data to be distributed into one or more blocks;
- defining an arbitrary numeric or alphanumeric indicator representing the level of security employed by the distribution process;
- producing a data size indicator representing at least the size of the block of data;
- producing an encoded data content indicator representing the unsegmented encoded information;
- producing an encoded checksum by performing a cyclic redundancy check operation on the file containing the encoded information;
- producing a block integrity verifier by performing a cyclic redundancy check operation on a file comprising the security indicator, the size indicator, the encoded data content indicator and the encoded checksum; and
- combining the security indicator, the size indicator, the encoded data content indicator, the encoded checksum and the block integrity verifier.

23. A process of installing software in a manner that prevents the unauthorized duplication or use of the software after it has been installed on a specific computer, wherein the process comprises:

- during the process of installation of the software onto the computer:
  - producing a unique identifier using information derived from the physical components of the workstation onto which the software is to be installed;
  - including the unique identifier into one or more of the files associated with the software as installed;
- at the time of initiation of execution of the software by a user after it has been installed;
  - producing a unique identifier using information derived from the physical components of the workstation onto which the software is to be installed;
  - comparing the unique identifier with a unique identifier included in one or more of the files associated with the software to executed; and
  - if the comparison provides a pre-defined negative result based on the unique identifiers, preventing the software from executing.

24. A process for preventing the installation or operation of software other than from a specified physical medium comprising:

- prior to encoding data onto a computer-readable medium wherein the data comprises files used to install the software, producing a unique identifier using information associated with the physical structure of the medium;
- including the unique identifier in one or more files used in the installation process for the said software;
- during the process of installation of the software,

- producing a unique identifier using information derived from the physical structure of the medium;
- comparing the unique identifier to the unique identifier included in the at least one file used in the installation process for the said software;
- if the comparison provides a pre-defined negative result based on the unique identifiers, causing the termination of the installation process.

25. The process as set forth in claim 24, wherein the information is secured by preventing the reading of data from the medium containing the software to be installed.

26. The process as set forth in claim 24, wherein the physical structure of the medium has been intentionally altered to incorporate a pre-defined arbitrary identifier.

27. The process as set forth in claim 26, wherein the medium is a floppy disk and the alteration is effected by permanently altering sectors of the disk to encode on said disk the pre-defined arbitrary identifier.

28. The process as set forth in claim 27, wherein the permanent alteration of said disk is effected by physically altering magnetic oxide residues on said disk which do not correspond to recorded bits on said disk.

29. The process as set forth in claim 28, wherein said permanent alteration is effected by using a laser to destroy said magnetic oxide residues.

30. A process of installing software across a network in a manner that prevents the unauthorized duplication or use of the software after it has been installed on a specific computer comprising:

- initiating an installation process for installing software onto a computer from a server computer using a network;
- producing a unique identifier using information derived from at least one physical component of the computer upon which the software is to be installed;
- including the unique identifier in at least one file associated with the software to be installed, wherein the absence of said file prevents operation of the software;
- transferring the files including at least the said file containing the included identifier to the computer upon which the software is to be installed;
- at the time of execution of the software after it has been installed,
  - producing a unique identifier using information derived from at least one physical component of the computer upon which the software is to be installed;
  - comparing the unique identifier to the unique identifier embedded in the said at least one file associated with the software;
  - if the comparison provides a pre-defined negative result based on the unique identifiers, preventing the software from executing, preventing the operation of the software.

31. The process as set forth in claim 30 wherein the identifier is produced on the server in response to said information.

32. The process as set forth in any one of claims 23, 24 or 30, wherein the process for producing the unique identifier further comprises:

- assigning an arbitrary identifier that uniquely identifies the producer of the software, the software product to be installed or the two factors in combination;
- producing a binary key by using the arbitrary identifier and information derived from at least one physical component of the computer upon which the software is to be installed in an algorithm that produces an exclusive and repeatable result.

33. The process according to any one of claims 14, 15, 22, 23, 24 or 30, wherein the information used to produce the key comprises an identifier permanently and uniquely associated with said component.

34. The process as set forth in claim 33, wherein the information unique to the component comprises descriptive data related to one or more physical or operational attributes of a hard drive.

35. The process as set forth in claim 33, wherein the information is selected from the group consisting of one or more of the following: the drive ATA information block, the drive partition table, the drive interface type, the drive data capacity in formatted state, the drive capacity in unformatted state, the number of cylinders on the drive, the number of sectors on each track, the diagnostic cylinder number, the drive defect map and the effective data transfer speed of the drive in bytes per second.

36. The process as set forth in claim 33, wherein the information unique to the component comprises one or more of the following: the system speed index; the DRAM refresh clocking value associated with the system board and BIOS of the computer; a unique serial number associated with the microprocessor; the information stored in a CMOS memory address above 16base10; the ROM table for the system; information obtained by parsing interrupt 1Ah of the system board; information obtained by parsing interrupt 15h of the system board; information representing the access time of a video port in the system in combination with the location of said video port on said system; information unique to specific circuits, adapters or devices attached to or embedded within the system, such as a network interface or an audio interface card.

37. The process as set forth in claim 33, wherein the identifier is produced from information associated with at least two components which is combined prior to being used to generate the binary key.

38. The process as set forth in claim 33, wherein the identifier is produced from information associated with at least three components which is combined prior to being used to generate the binary key.

39. The process as set forth in claim 33, wherein the identifier is produced from information associated with at least four components which is combined prior to being used to generate the binary key.

40. The process as set forth in claim 33, wherein the identifier is produced from information associated with at least five components which is combined prior to being used to generate the binary key.

41. The process as set forth in claim 33, wherein the identifier is produced from information associated with at least six components which is combined prior to being used to generate the binary key.

42. The process as set forth in claim 33, wherein the identifier is produced from information associated with at least seven components which is combined prior to being used to generate the binary key.

43. A process for securely distributing information representing an audio or audiovisual work comprising:

- producing a binary key using information derived from at least one physical component of a device capable of rendering the work;
- associating with the information representing the audio or audiovisual work the binary key produced;
- distributing the information to the location at which the information is to be rendered;
- prior to or during the rendering of the information on a device capable of rendering said information,
  - producing a binary key using information derived from at least one physical component of the device;
  - retrieving from said information the binary key associated with said information;
  - comparing the binary key extracted from said information with the binary key produced using information from the device;
  - preventing the rendering of the information if the binary key associated with the information is not identical to the binary key produced using the device.

44. The process as set forth in claim 43, wherein the device is selected from the group consisting of a general purpose computer, a special purpose computer, a DVD player, a CD player, a motion picture projector or a device that comprises a video display unit in combination with circuitry capable of rendering an audiovisual work in a digital form.

45. The process as set forth in claim 44, wherein the component is a device attached to the lens of a motion picture projector and the device comprises a circuit and elements that are capable of altering or preventing the display of images by the projector.

46. The process as set forth in any one of claims 43, 44 or 45, which further comprises:

- producing a binary key using attributes of a device that can be attached to the lens of a motion picture projector;
- encoding the binary key into the information as encoded onto a medium suitable for distribution and use in motion picture rendering of audiovisual works;
- during the rendering of said information, extracting from said information the binary key;

- producing a binary key using information from a component attached to the lens of a motion picture projector; and
- comparing the binary key produced from said component to the binary key extracted from the information,

47. The process as set forth in any one of claims 44 or 45, wherein the binary key is encoded onto the audio track of the audiovisual work.

48. The process as set forth in claim 47, wherein the binary key is encoded by placing an audio signal into one or more spectrums of the audio track of the audiovisual work.

49. The process as set forth in claim 48, wherein the binary key is encoded into the audio track of the audiovisual work using tones in sub-audio, supra audio and audio frequencies.

50. The process as set forth in any one of claims 43, 44, 45, 46, 47, 48 or 49, wherein the rendering is prevented by blocking or altering the projection of images through the lens of a motion picture projector.

51. The process as set forth in any one of claims 43, 44, 45, 46, 47, 48 or 49, wherein the rendering is prevented by disabling the operation of the motion picture projector.

52. The process as set forth in any one of claims 43, 44, 45, 46, 47, 48 or 49, wherein the rendering is prevented by blocking the supply of electricity to the device that is to render the information.

53. The process as set forth in any one of claims 43, 44, 45, 46, 47, 48 or 49, wherein the rendering is prevented by blocking the transmission of a video signal to a display.

54. A process of preventing the unauthorized rendering of information originally stored on an optically readable medium, wherein the process comprises:

- defining a unique identifier for the information to be secured;
- incorporating a unique physical media identifier into the physical structure of the optically readable medium;
- producing a binary key of at least 128 bits using the unique identifier for the information to be secured and the physical media identifier;
- encoding the binary key on the optical medium in a form readable by a device that can render the information;
- prior to or during the rendering of the information by the device;
  - causing the device to evaluate the physical media to detect the binary key and the unique physical media identifier;
  - evaluating the information obtained by the detection step to determine if the information to be rendered is encoded on the optical medium having the unique physical media identifier;

- if the evaluation step provides a pre-defined negative result, preventing the device from rendering the encoded information.

55. The process as set forth in claim 54, wherein the encoding of the binary key and the unique physical media identifier is effected by physically altering a portion of the optical medium outside that used to store data representing information to be rendered.

56, The process as set forth in claim 54 wherein the device comprises a CD-player, a DVD-player or a videodisc player.

57. The process as set forth in claim 55, wherein the binary key is encoded on the surface of the optical medium using a physical structure distinct from that used to encode data representing information to be rendered on said structure.

58. The process as set forth in claim 57, wherein the data as encoded in the physical structure is to be read by a laser at an angle other than 90 degrees.

59. The process as set forth in claim 55, wherein the device detects the binary key and the unique physical media identifier by evaluating a circuit attached to or embedded within the optical medium.

60. The process as set forth in claim 55, wherein the unique physical media identifier and the binary key are stored in a circuit embedded within the optical medium and the device reads the information in said circuit by activating the circuit upon contact with the device.

61. The process as set forth in claim 55, wherein the unique physical media identifier and the binary key are stored in a circuit attached to the spindle hole of the optical medium.

62. The process as set forth in claim 55, wherein the binary key and the unique physical media identifier are encoded in the inner side surface of the spindle hole of the optical medium in a form that may be read by optical or magnetic means located within the device that is to render the encoded information.

63. A process for preventing the unauthorized rendering of a audiovisual or audio work in a digital form, wherein the process comprises:

- producing a binary key using information derived from at least one physical component of a device capable of rendering the work;
- encoding the information representing the audio or audiovisual work using an algorithm in conjunction with the binary key so produced;
- distributing the information to the location at which the information is to be rendered;
- prior to or during the rendering of the information on a device capable of rendering said information,
  - producing a binary key using information derived from at least one physical component of the device;
  - decoding the encoded information using the binary key produced;

- rendering the decoded information.

64. The process according to claim 63, wherein the decoding of the encoded information is performed contemporaneously with the rendering of the information.

65. The process according to claim 64, wherein the binary key is unique to a specific device.

66. The process according to claim 64, wherein the binary key is unique to a class of devices that share a commonly identifiable component that is used to generate said key.